UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
[redacted]
Columbus, Ohio 43201

Case No. 1:22-mj-477

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A-1

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 111, 930, and 1361	Assault, Intimidation, or Impeding of Officers; Bringing Firearms onto Federal Property; Damage to Federal Property

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attach

[redacted]

[redacted]

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by via FaceTime video *(specify reliable electronic means).*

Date: Aug 11, 2022

Karen L. Litkovitz
United States Magistrate Judge

City and state: _____

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF: [redacted] Columbus, Ohio 43201; and 2003 Ford Crown Victoria with FL license plate: [redacted]	Case No. 1:22-mj-477

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, [redacted] being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search: (1) the premises known as [redacted], Columbus, Ohio 43201, hereinafter "PREMISES," further described in Attachment A-1, for the things described in Attachment B; and (2) a 2003 Ford Crown Victoria with Florida license plate [redacted] hereinafter the "VEHICLE," further described in Attachment A-2, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since January of [redacted] I completed the training requirements to become an FBI agent in [redacted] at Quantico, Virginia. During that training, I learned how to investigate firearms offenses, controlled substance offenses, white collar crimes, and other violations of federal law. I

am currently assigned to the Joint Terrorism Task Force (JTTF) squad at the FBI [redacted] Field Office. My duties include conducting criminal investigations involving violations of federal law contained in Title 18 and Title 21 of the United States Code.

3. [redacted]

4. I have participated in the execution of federal search warrants and federal arrest warrants in relation to investigations into domestic terrorism, organized crime, financial fraud, and violent crimes to include prohibited possession of firearms, the unlawful possession, possession with the intent to distribute, and actual distribution of controlled substances, as well as the associated conspiracies in violation of Title 21, United States Code, Sections 841(a)(1) and 846. I have also been involved with the seizure and review several cellular devices, computers, storage media, and other digital media devices for relevant evidence in connection to these investigations.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. This investigation pertains to alleged violations of 18 U.S.C. 111 (assault, intimidation, or impeding of officers), 18 U.S.C. 930(b) (possession of firearm at federal facility), and 18 U.S.C. 1361 (damage to federal property), those violations involving suspect Ricky W. Shiffer, Jr. and occurring on or about August 11, 2022 in the Southern District of Ohio.

PROBABLE CAUSE

7. On or about August 11, 2022, Protective Security Officers ("PSO") with Paragon assigned to the Federal Bureau of Investigation [redacted] Ohio Division Headquarters City ("FBI [redacted] HQC") located at [redacted] Ohio 45236, were stationed in the Visitor Screening Facility ("VSF") at the front of the FBI [redacted] HQC building. Between approximately 9:00 and 9:15 a.m., PSO Officers observed a white vehicle (the "VEHICLE") quickly pull into the VSF parking lot. A white male, described as wearing a short-sleeved shirt, approximately 5'10" to 6'0" in height, having a slender to medium build, bald, and without any facial hair, later identified as Ricky Walter Shiffer, Jr. (the "SUBJECT"), exited the vehicle with an AR-15 style rifle slung across his body and carrying a nail gun. PSO Officers also observed the SUBJECT wearing some type of vest. The SUBJECT then approached the VSF and attempted to use a nail gun on the one of the VSF windows. At approximately 9:11 a.m., PSO Officers activated an internal security alarm.

8. After multiple attempts to use the nail gun on a VSF window, the SUBJECT returned to his vehicle and drove the vehicle through the VSF parking lot and departed the VSF parking lot.

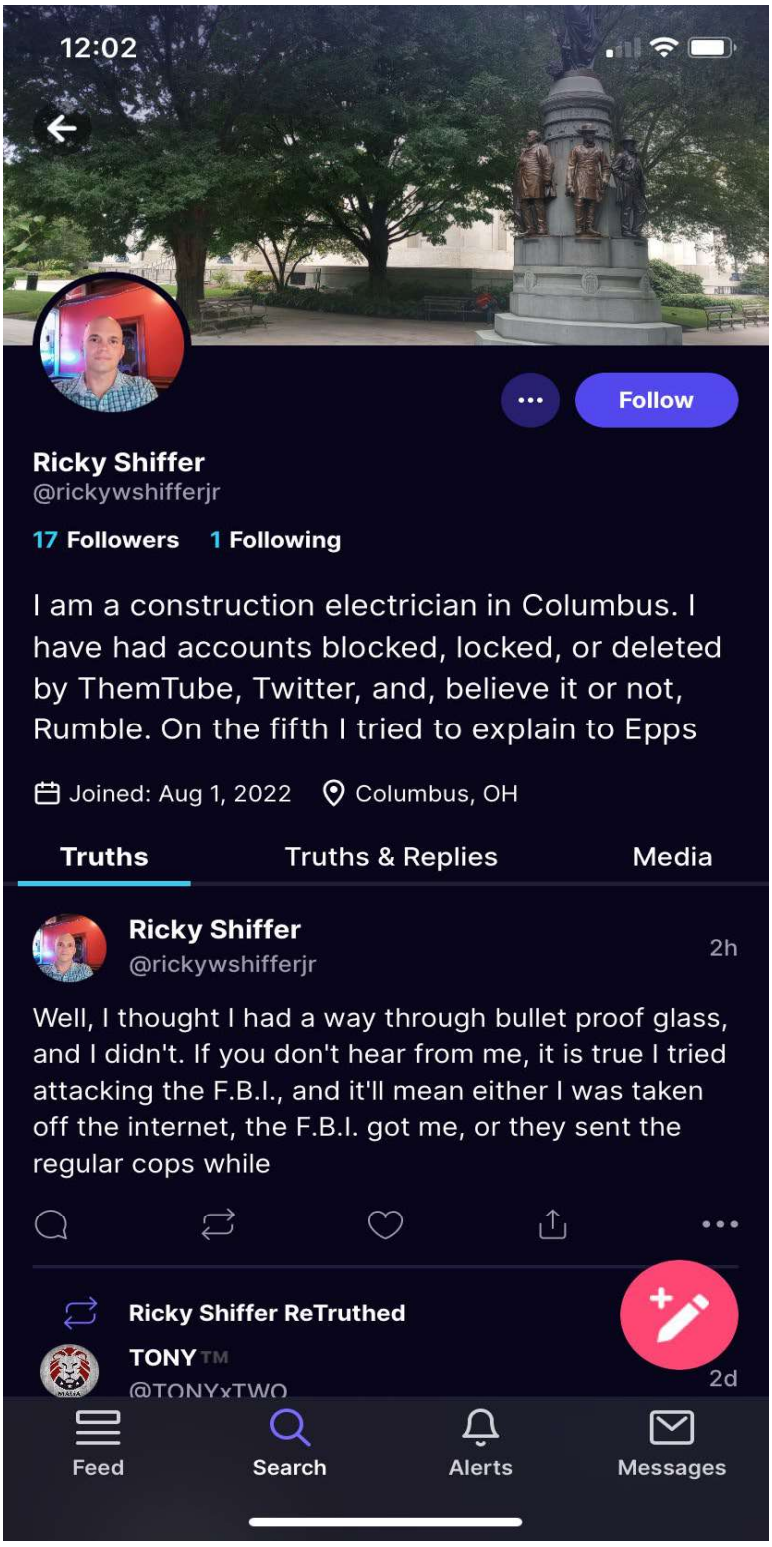
9. The VEHICLE had a Florida license plate of [redacted] Florida Bureau of Motor Vehicle records show the VEHICLE as being registered to the SUBJECT.

10. Between approximately 9:35 and 9:40 a.m., responding federal Agents followed the SUBJECT in the VEHICLE northbound on Interstate 71. Agents contacted a Captain with the Ohio State Highway Patrol ("OSP") for assistance. OSP Officers joined the pursuit with Agents.

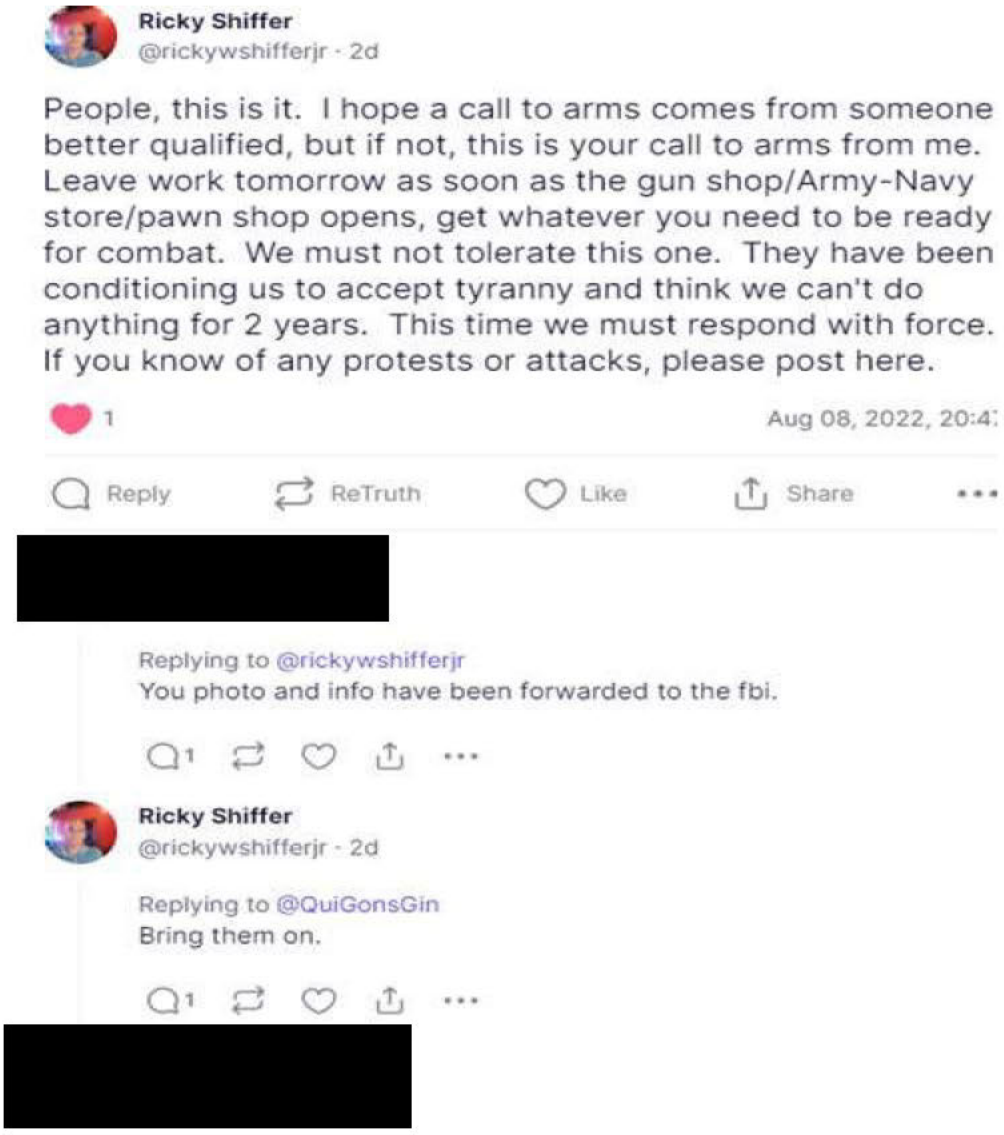
11. At some point during the pursuit, a vehicle stop of the VEHICLE was initiated. The SUBJECT then began firing shots at law enforcement and fled in the VEHICLE.

12. At approximately 10:06 a.m., the SUBJECT was observed by responding Agents and officers outside of and adjacent to the VEHICLE with a weapon near the intersection of Smith Road and Van Tress Road in or near Wilmington, Ohio. Agents reported that shots were exchanged between law enforcement and the SUBJECT. The armed SUBJECT remained in a standoff with law enforcement from approximately 10 a.m. though approximately 4 p.m. At the conclusion of the standoff with law enforcement, the SUBJECT was deceased.

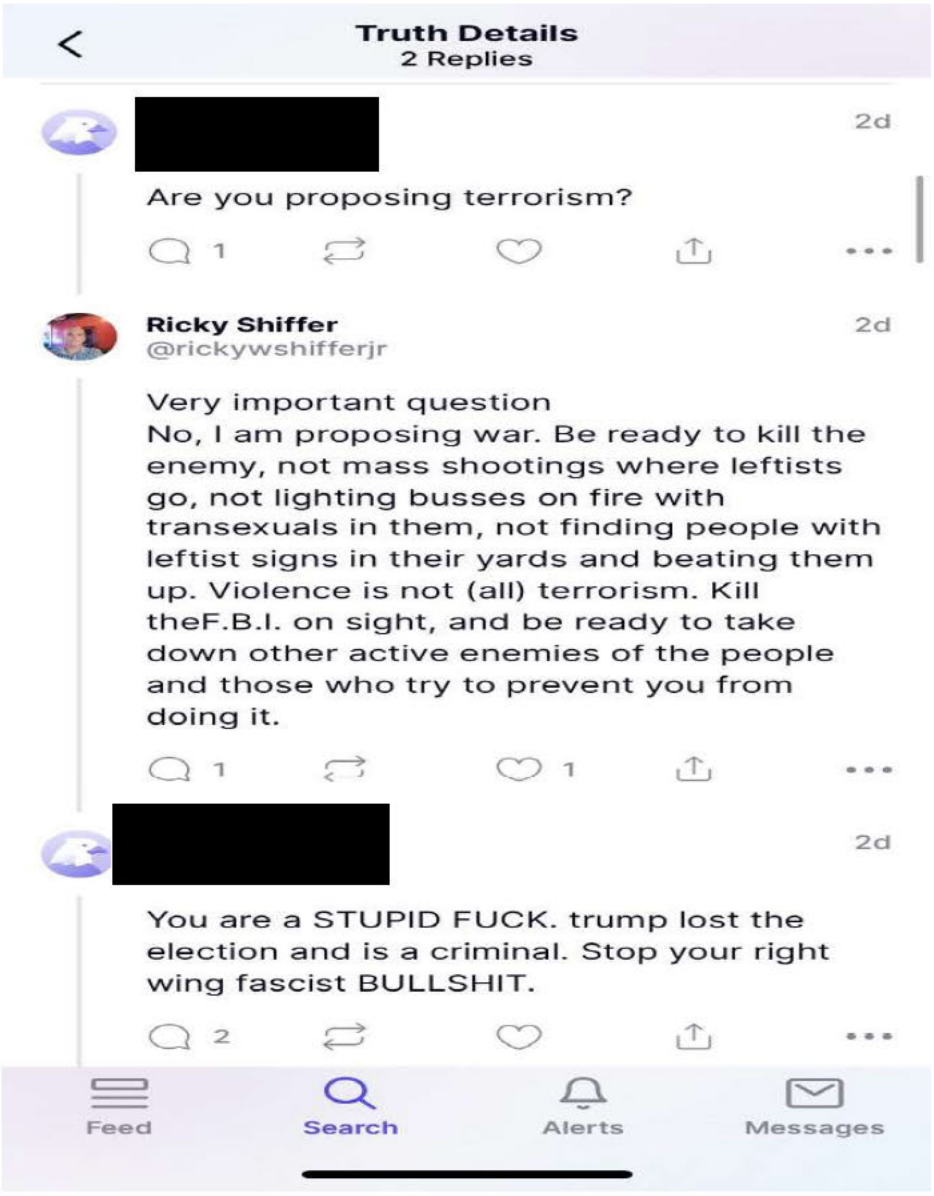
13. Investigators identified a Truth Social account with profile name "Ricky Shiffer" and username @rickywshifflerjr. At some point during the standoff, a post was made to the account relating to the events at the FBI [redacted] HQC on August 11, 2022, as shown below:


12:02
Follow
Ricky Shiffer
@rickywshifferjr
17 Followers 1 Following
I am a construction electrician in Columbus. I have had accounts blocked, locked, or deleted by ThemTube, Twitter, and, believe it or not, Rumble. On the fifth I tried to explain to Epps
Joined: Aug 1, 2022
Columbus, OH
Truths
Truths & Replies
Media
Ricky Shiffer
@rickywshifferjr
2h
Well, I thought I had a way through bullet proof glass, and I didn't. If you don't hear from me, it is true I tried attacking the F.B.I., and it'll mean either I was taken off the internet, the F.B.I. got me, or they sent the regular cops while
Ricky Shiffer ReTruthed
TONY
2d
Feed
Search
Alerts
Messages

14. Investigators located a Truth Social post made to the @rickywshifflerjr account on or about August 8, 2022 discussing a "call to arms" and that people must respond to "this one" with force, as shown below. The August 8, 2022 date corresponds to day the FBI executed a search warrant on Former President Donald Trump's Mar-a-Lago residence.



15. Investigators located what appears to be a reply made to the Truth Social post above, where another Truth Social user asked @rickywshefflerjr if he was proposing terrorism. A reply from @rickywshefflerjr indicated that he was proposing war, not terrorism, and that people need to be ready to kill the FBI "on sight."



16.

17. On or about August 11, 2022, investigators confirmed through the apartment manager at the PREMISES that the SUBJECT signed a lease at the PREMISES in April 2022 and is currently occupying the PREMISES.

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

19. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES and in the VEHICLE, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

20. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES or in the VEHICLE, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES or VEHICLE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the

computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the

computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence

of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

22. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

24. I submit that this affidavit supports probable cause for a warrant to search the PREMISES and the VEHICLE, described in Attachments A-1 and A-2, and seize the items described in Attachment B.

25. The FBI further advises that other state agencies, including Ohio Bureau of Criminal Investigation, may be involved in and assisting with the processing of evidence in this matter.

REQUEST FOR SEALING

26. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

[redacted]

Federal Bureau of Investigation

Subscribed and sworn to before me
on August 11, 2022:

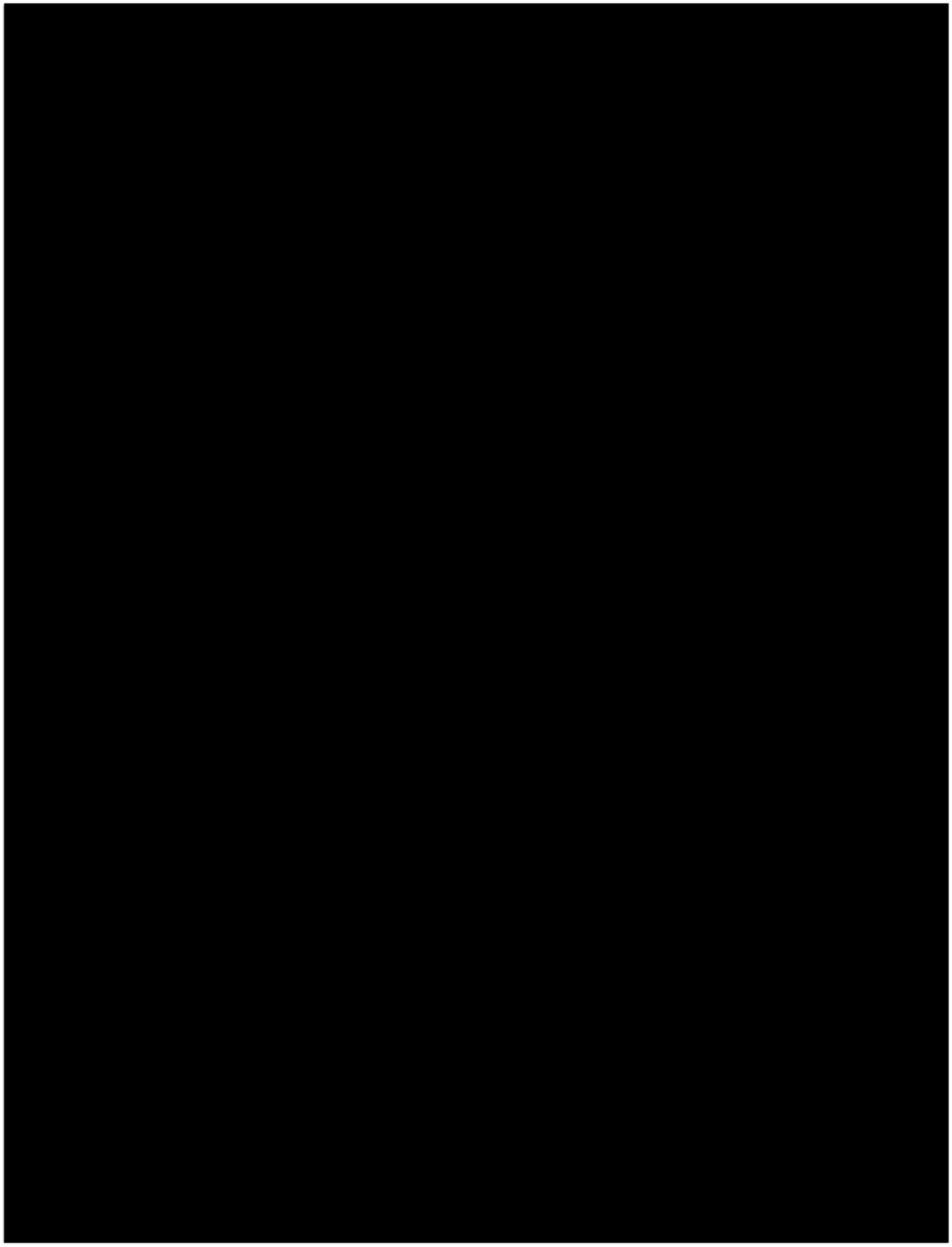
Karen L. Litkovitz
United States Magistrate Judge

ATTACHMENT A-1 (APARTMENT)

Property to be searched

The property to be searched is [redacted] Columbus, Ohio 43201, further described as a brick apartment building. Photographs of the building and entrance are below.

[redacted]



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. 111 (assault, intimidation, or impeding of officers), 18 U.S.C. 930(b) (possession of firearm at federal facility), and 18 U.S.C. 1361 (damage to federal property), those violations involving suspect Ricky W. Shiffer, Jr. and occurring on or about August 8, 2022 to the present, including:

a. Items used for an attack or assault, including firearms, ammunition, nail guns (and related equipment), body armor, helmets, and masks;

b. Records and information relating to items used for a violent attack or assault, including firearms, ammunition, nail guns (and related equipment), body armor, helmets, and masks;

c. Records and information relating to communication devices, including phones and computers, used in the planning, preparation or in furtherance of the attack on August 11, 2022;

d. Records and information relating to the Federal Bureau of Investigation, including but not limited to, research or websites about the location of the FBI offices, FBI investigations, FBI security measures or other operational security;

e. Records and information relating to the suspect's motive and intent; and

f. Records and information relating to any associates of the suspect relating to the offenses above.

2. Computers, devices, or storage media used as a means to commit or facilitate the violations described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
[redacted]
Columbus, Ohio 43201

Case No. 1:22-mj-477

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of Ohio
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A-1

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

YOU ARE COMMANDED to execute this warrant on or before 8/25/2022 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Karen L. Litkovitz/Hon. Stephanie K. Bowman .
(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
❒ for ____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of ____ .

Date and time issued: 6:58 PM, Aug 11, 2022

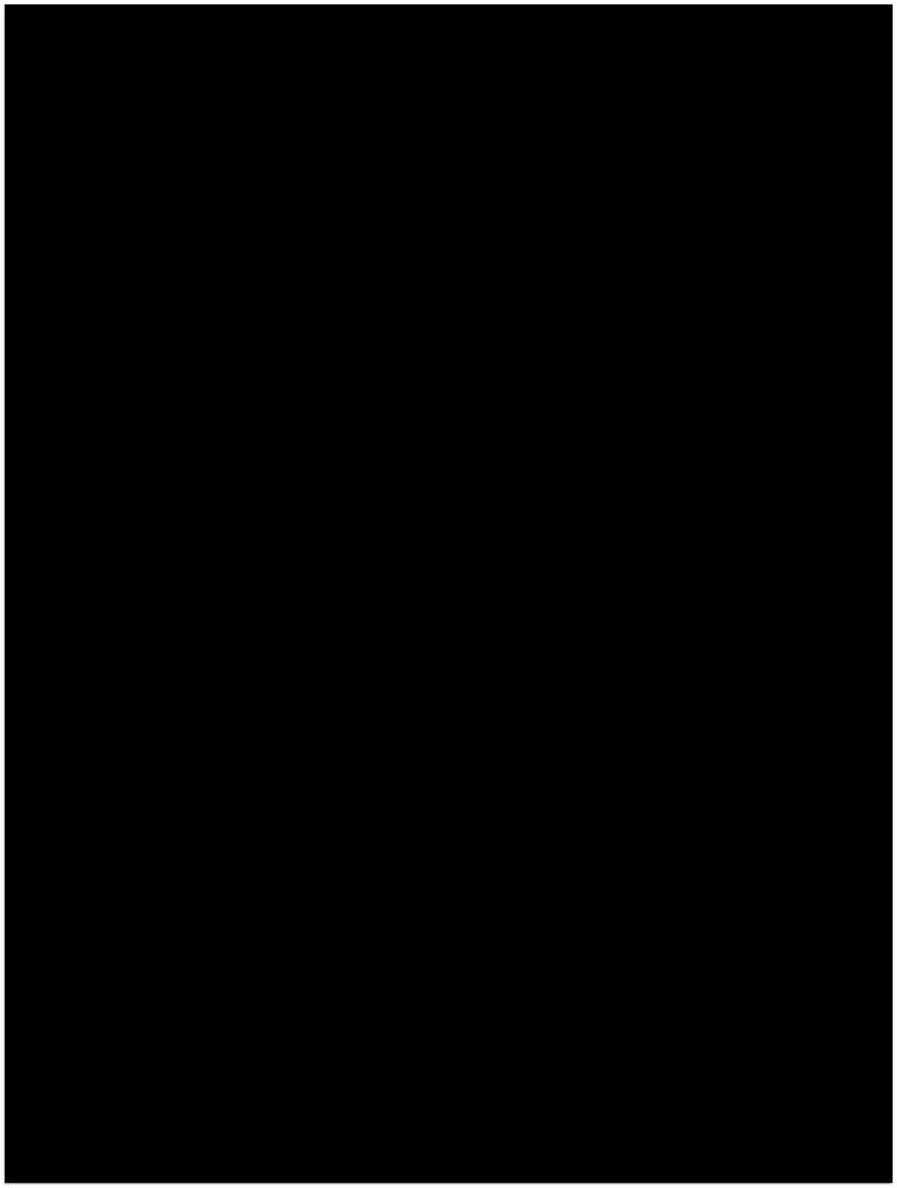
Karen L. Litkovitz
United States Magistrate Judge

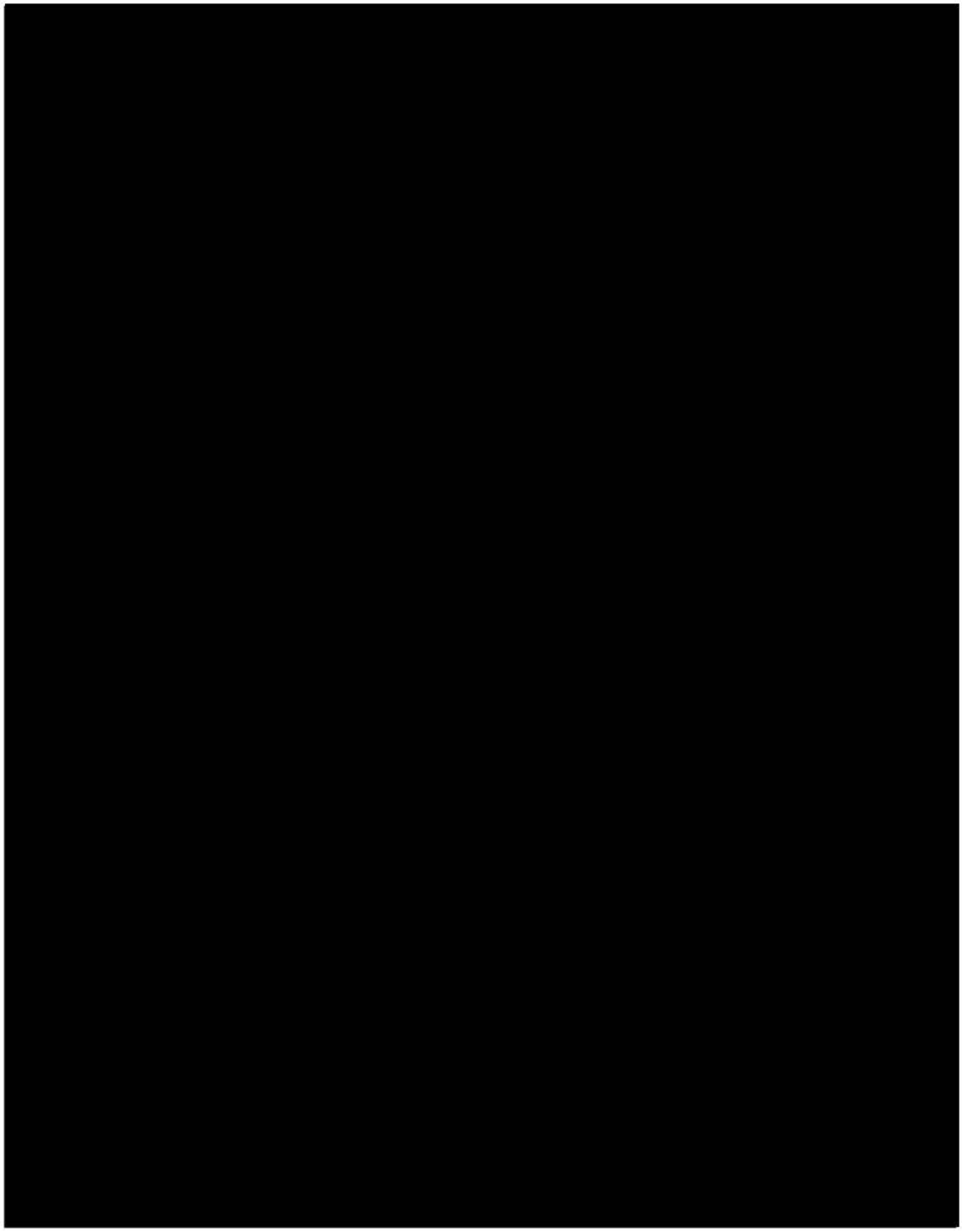
City and state: Cincinnati, OH

ATTACHMENT A-1 (APARTMENT)

Property to be searched

The property to be searched is [redacted] Columbus, Ohio 43201, further described as a brick apartment building. Photographs of the building and entrance are below.





ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. 111 (assault, intimidation, or impeding of officers), 18 U.S.C. 930(b) (possession of firearm at federal facility), and 18 U.S.C. 1361 (damage to federal property), those violations involving suspect Ricky W. Shiffer, Jr. and occurring on or about August 8, 2022 to the present, including:

a. Items used for an attack or assault, including firearms, ammunition, nail guns (and related equipment), body armor, helmets, and masks;

b. Records and information relating to items used for a violent attack or assault, including firearms, ammunition, nail guns (and related equipment), body armor, helmets, and masks;

c. Records and information relating to communication devices, including phones and computers, used in the planning, preparation or in furtherance of the attack on August 11, 2022;

d. Records and information relating to the Federal Bureau of Investigation, including but not limited to, research or websites about the location of the FBI offices, FBI investigations, FBI security measures or other operational security;

e. Records and information relating to the suspect's motive and intent; and

f. Records and information relating to any associates of the suspect relating to the offenses above.

2. Computers, devices, or storage media used as a means to commit or facilitate the violations described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite"

web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: ____________________

____
Executing officer's signature

____
Printed name and title